UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,717	05/14/2001	Roy Cohen	Q01 /3	6616

7590 11/16/2004

Dr. Mark M. Friedman
c/o Discovery Dispatch
9003 Florin Way
Upper Marlboro, MD 20772

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/853,717	COHEN, ROY	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 May 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

Drawings

2. The drawings (Figures 2 and 3) are objected to as failing to comply with 37 CFR 1.84(u)(1) because they need to be labeled as 2A, 2B, 3A, 3B. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claim 17 is objected to because of the following informalities: "stegnography" should be "steganography". Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-2, 7, 9-13 are rejected under 35 U.S.C. 102(b) as being anticipated by Hulme ("Cryptography" January 3, 1899).

As per claim 1, Hulme discloses a method for scrambling data according to a map, the data being composed of a plurality of units of data in a particular sequence, the method comprising: selecting a plurality of points in a particular order to form the map; and scrambling the sequence of the units of data according to the map to form scrambled units of data such that the map is required lo unscramble said scrambled units of data, and such that said scrambled units of data are not readable without the map (see page 155).

As per claim 2, Hulme discloses the map being manually created by a user (see page 155).

As per claim 7, Hulme discloses the units of data are collected into a file, such that said file is divided into a plurality of fragments, and such that an order for assembling said plurality of fragments is determined by the map (see pages 159-163).

As per claim 9, Hulme discloses the file is divided into the plurality of fragments before the units of data are scrambled, such that the units of data are scrambles at least within each fragment (see pages 159-163).

As per claim 10, Hulme discloses the units of data are scrambled between the plurality of fragments (see pages 159-163 where the rotation of the map is this scrambling).

As per claim 11, Hulme discloses a correct order of said plurality of fragments is determined according to the map, such that without the map, said plurality of fragments cannot be reassembled in said correct order (see pages 159-163).

As per claim 12, Hulme discloses the units of data are encrypted according to a key, said key being obtained from the map (see pages 159-163 where the map is the key).

As per claim 13, Hulme discloses the key is a plurality of keys, each key being used to scramble or encrypt a portion of the units of data (see pages 159-163).

6. Claims 1-2, 6 are rejected under 35 U.S.C. 102(b) as being anticipated by British War Office ("Manual of Cryptography").

As per claim 1, British War Office discloses a method for scrambling data according to a map, the data being composed of a plurality of units of data in a particular sequence, the method comprising: selecting a plurality of points in a particular order to form the map; and scrambling the sequence of the units of data according to the map to form scrambled units of data such that the map is required lo unscramble said scrambled units of data, and such that said scrambled units of data are not readable without the map (see pages 93-94).

As per claim 2, British War Office discloses the map being manually created by a user (see pages 93-94).

As per claim 6, British War office discloses drawing the map by said user, such that points from the map are used to scramble the data (see pages 93-94).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hulme as applied to claim 2 above, and further in view of Novaes (U.S. 6,460,068).

As per claim 3, Hulme fails to disclose displaying a fractal to the user and the user selecting points from the fractal to form the map.

However, Novaes teaches choosing points from a fractal to form a map (see column 7 lines 36-44 where figures 10A-10C are the map).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Novaes' method of forming a map to create the map of Hulme.

Motivation to do so would have been to create a map from expansions of the fractals (see column 1 lines 11-25).

As per claim 4, the modified Hulme and Novaes method discloses the user also selects at least one of a resolution, the coordinates of the first navigation point for the map and the color bar code for the fractal (see Novaes column 7 lines 36-44 and figures 10A-10C where the first navigation point is seen in the figures).

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hulme as applied to claim 7 above, and official notice has been taken that it would have been obvious to one skilled in the art to divide the file into fragments after the units of data are scrambled. Motivation to do so would have been to allow the fragments to take separate paths to a destination.

10. Claims 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hulme as applied to claim 13 above, and further in view of Menezes et al ("Handbook of Applied Cryptography").

As per claim 14, Hulme fails to disclose each key is used in sequential order to encrypt a subsequent key in the sequential order.

However, Menezes et al teaches such a method (see page 497 where K is the first key and r_A is the subsequent key).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's method for key transportation with Hulme's encryption technique.

Motivation to do so would have been to update a key (see page 497 (i)).

As per claim 15, the modified Hulme and Menezes et al method discloses plurality of encrypted keys are used in said sequential order for communication between at least two users, such that a first user sends a first key to said second users and such that each decrypted key is used to scramble data for transmission between said at first two users (see Menezes page 497).

11. Claims 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hulme and further in view of Sasich et al (U.S. 6,661,904).

As per claim 22, Hulme discloses the use of a map for scrambling data being operated by a user (see page 155).

Hulme fails to disclose this being done in a software module at a computational device and a server for receiving the scrambled data from the user computational device and a network connected to said server and the user computations device for transmitting the data.

However, Sasich et al teaches a computational device for scrambling data (see column 6 lines 25-29 where embedding data scrambles it) and a server for receiving scrambled data via a network (see column 14 lines 12-34).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Sasich et al's system with a server, a computational device, and a network connecting them.

Motivation to do so would have been to electronically transmit data.

As per claim 23, the modified Hulme and Sasich et al system discloses the software module also conceals said scrambled data in at least one image (see Sasich et al column 6 lines 25-29), said at least one image being stored by said server (see column 14 lines 12-34).

As per claim 24, the modified Hulme and Sasich et al system discloses the scrambles data is concealed in a plurality of images, and wherein each image contains both a portion of said scrambles data and a location of a subsequent image for obtaining a subsequent portion of said scrambled data (see column 6 lines 25-29).

12. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hulme and Novaes method as

applied to claim 3 above, and further in view of Hoffberg et al (U.S. 5,774,357).

As per claim 5, the modified Hulme and Novaes method fails to disclose removing colors from the fractal.

However, Hoffberg et al discloses removing colors from an image (see column 74 lines 49-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Hoffberg et al's method of removing colors on the modified Hulme and Novaes method.

Motivation to do so would have been to make it easier to extract the characters (in this case the map) (see column 74 lines 49-67).

13. Claims 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hulme and Menezes et al method as applied to claim 15 above, and further in view of Sasich et al (U.S. 6,661,904).

As per claim 16, the modified Hulme and Menezes et al method fails to disclose the plurality of encrypted keys also includes information about a location for storing data as well as at least a portion of a map for unscrambling said data, such that said second user sequentially locates and unscrambles said data according to each decrypted key.

However Sasich et al teaches embedding data including the location of the next set of data (see column 6 lines 25-29).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Sasich et al's method of embedding location data to define locations for the sequential keys of the modified Hulme and Menezes et al method.

Motivation to do so would have been to prevent degradation of the image the embedded data is being stored in (see Sasich et al column 6 lines 25-29).

As per claim 17, the modified Hulme, Menezes et al, and Sasich et al method discloses the scrambled units of data are concealed in an image by steganography (see Sasich et al column 6 lines 25-29).

As per claim 18, the modified Hulme, Menezes et al, and Sasich et al method discloses the scrambled units of data are divided into a plurality of groups, and each group is concealed in a separate image (see Sasich et al column 6 lines 25-29).

As per claim 19, the modified Hulme, Menezes et al, and Sasich et al method discloses the separate image also contains information for locating another group in another image, such that said groups are concealed in a plurality of sequential images (see Sasich et al column 6 lines 25-29).

14. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hulme and Sasich et al system as applied to claim 24 above, and further in view of Schneier ("Applied Cryptography").

As per claim 25, the modified Hulme and Sasich et al system fails to disclose the server destroys said portion of said scrambled data after said portion of said scrambled data is accessed.

However, Schneier discloses destroying data (see pages 228-229).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's method of destroying data in the modified system Hulme and Sasich et al.

Motivation to do so would have been to keep the information secret.

15. Claims 20-21 rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hulme, Menezes et al, and Sasich et al method as applied to claim 19 above, and further in view of Bocionek et al (U.S. 6,301,360).

As per claim 20, the modified Hulme, Menezes et al, and Sasich et al method fails to disclose each image is a fractal.

However, Bocionek et al discloses using a fractal to embed data (see column 6 lines 55-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Bocionek et al's fractal as the sequential images of the modified Hulme, Menezes et al, and Sasich et al method.

Motivation to do so would have been the added security of needing to know the parameters of the chaotic function used to create the fractal (see Bocionek et al column 7 lines 10-18).

As per claim 21, the modified Hulme, Menezes et al, Sasich et al, and Bocionek et al method discloses a visual appearance of said image is altered according to a visual effect for further concealing said data (see Sasich et al column 6 lines 40-51).

16. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hulme, Sasich et al, and Schneier system as applied to claim 25 above, and further in view of Bocionek et al (U.S. 6,301,360).

As per claim 26, the modified Hulme, Sasich et al, and Schneier system fails to disclose each image is a fractal.

However, Bocionek et al discloses using a fractal to embed data (see column 6 lines 55-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Bocionek et al's fractal as the sequential images of the Hulme, Sasich et al, and Schneier system.

Motivation to do so would have been the added security of needing to know the parameters of the chaotic function used to create the fractal (see Bocionek et al column 7 lines 10-18).

17. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hulme, Sasich et al, Schneier and Bocionek et al system as applied to claim 26 above, and further in view of Menezes et al.

As per claim 27, the modified Hulme, Sasich et al, Schneier and Bocionek et al system fails to disclose a plurality of user computational devices, such that said server stores a plurality of keys, each key being assigned to a user computational device, and such that said sewer scrambles each key according to a key of another user computational device to transmit said first key to said other user computational device.

However, Menezes et al teaches such a system (see pages 546-547).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's

system for distributing keys in the modified Hulme, Sasich et al, Schneier and Bocionek et al system.

Motivation to do so would have been to efficiently distribute keys (see Menezes et al page 546).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

Andrew Caldwell
Andrew Caldwell